

FILED ENTERED
LODGED RECEIVED

FEB 19 2009 RE

AT SEATTLE
CLERK U.S. DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
BY DEPUTY



09-CV-00216-CMP

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

LAURA KROTTNER,

Plaintiff,

v.

STARBUCKS CORPORATION, a Washington
Corporation,

Defendant.

No. **C09-0216** RAJ

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

I. INTRODUCTION

Plaintiff Laura Krottner ("Plaintiff"), on behalf of herself and all others similarly situated, alleges the following against the above-captioned Defendant, based upon personal knowledge, where applicable, and on information and belief and the investigation and research of counsel.

II. NATURE OF THE ACTION

1. Plaintiff brings this class action suit on her own behalf, and on behalf of all entities and persons similarly situated, against Starbucks Corporation ("Starbucks"), as a result of its failure to adequately safeguard its employees' sensitive, personal information (hereinafter "Personally Identifiable Information" or "PII").

NO Summons Issued SEA 24082

1 2. As a result of Starbucks's failure to adequately protect and secure Plaintiff's and
2 Class Members' PII, unauthorized individuals stole a laptop containing access to Plaintiff's and
3 Class Members' PII (hereinafter the "Breach"). Here, the PII stolen during the Breach contained
4 names, addresses, and social security numbers of approximately 97,000 Starbucks employees.

5 3. In this electronic age, it is standard practice to encrypt sensitive personal and
6 financial information, such as the PII of employees, in order to protect such information from
7 both internal and external threats. Defendant's failure to maintain reasonable and adequate
8 security procedures to protect against the theft of Plaintiff's and the Class Members' PII has put
9 Plaintiff and the Class Members at an increased and imminent risk of becoming victims of
10 identity theft crimes, fraud, and abuse. In addition, Plaintiff and the Class have spent (or will
11 need to spend) considerable time and money to protect themselves as a result of Defendant's
12 conduct.

13 4. Plaintiff and the Class will suffer irreversible damage if and when their PII
14 becomes misused. As a proximate result of the Breach, thousands of Starbucks employees,
15 including Plaintiff, have had their PII compromised, their privacy invaded, have been deprived of
16 the exclusive use and control of their PII, have incurred out-of-pocket costs, loss of time, and
17 have otherwise suffered economic damages in order to consistently monitor their credit card
18 accounts, credit reports, and other financial information in order to protect their PII from
19 imminent misuse.

20 III. JURISDICTION AND VENUE

21 5. This Court has subject matter jurisdiction over this action pursuant to the Class
22 Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because Plaintiff is of diverse citizenship
23

1 from Defendant; there are more than 100 Class Members nationwide; and the aggregate amount
2 in controversy exceeds \$5,000,000, excluding interest and costs.

3 6. This Court has personal jurisdiction over the parties because Defendant conducts
4 substantial business in this state, has systematic and continuous contacts with this state, and has
5 agents and representatives that can be found in this state.

6 7. Venue is appropriate under the authority of 28 U.S.C. § 1391(b) because the
7 Defendant resides in this District and/or a substantial part of the challenged actions took place
8 and/or emanated from this District.

9
10 **IV. PARTIES**

11 8. Plaintiff Laura Krottner is a resident of Chicago, Illinois. She has been a
12 Starbucks employee for three years and received notice from Defendant that her PII may have
13 been breached.

14 9. Defendant Starbucks Corporation (NasdaqGS: SBUX) (hereinafter "Starbucks",
15 "Company" or "Defendant") is the world's leading roaster and retailer of specialty coffee,
16 incorporated and headquartered in the State of Washington. Starbucks's corporate address is
17 2401 Utah Avenue South, Seattle, Washington 98134. At the fiscal end of 2008, Starbucks
18 operated 7,463 locations worldwide with 4,329 of those locations operating in the United States.
19 Starbucks employs approximately 176,000 people worldwide. In the United States, Starbucks
20 employs approximately 143,000 people, with 136,000 in Company-operated retail stores. The
21 remainder of the employees work in the Company's administrative and regional offices, store
22 development, roasting and warehousing operations. Approximately 33,000 employees are
23 employed outside of the United States, with 32,000 in Company-operated retail stores. The
24
25
26

1 remainder work in the Company's regional support facilities and roasting and warehousing
2 operations.

3 V. FACTUAL ALLEGATIONS

4 10. Starbucks, an international retailer of coffee and coffee beans, employs
5 approximately 176,000 people globally.

6 11. On or about October 29, 2008, a Starbucks laptop, containing the PII of
7 approximately 97,000 Starbucks employees, was stolen from an unspecified location.

8 12. The stolen PII contained names, addresses, and social security numbers.

9 13. Starbucks sent a letter to at least some of those affected, dated November 19,
10 2008, and signed by Russell Walker, VP, Enterprise Security, Starbucks Coffee Company
11 (hereinafter "Notice Letter") (attached hereto as Exhibit A). The Notice Letter stated that
12 Starbucks Enterprise Security learned that a laptop containing employee information was stolen
13 on October 29, 2008, and that Plaintiff's PII was compromised in the theft of the laptop.
14

15 14. Upon information and belief, the PII data itself was unencrypted.

16 A. The Data Breach

17 15. On or about October 29, 2008, a laptop owned by Starbucks and containing the
18 PII of approximately 97,000 Starbucks employees was stolen.
19

20 16. Starbucks has not revealed where the laptop containing the PII was stolen from,
21 but according to the Wisconsin Department of Agriculture "[a] laptop containing personal
22 information was stolen from the corporate facility." Trade and Consumer Protection, Office of
23 Privacy Protection's website, <http://privacy.wi.gov/databreaches/2008/nov08.jsp> (last visited Jan.
24 10, 2009).
25
26

1 17. In a letter to Maryland Attorney General Douglas Gansler, Starbucks stated that
2 they will continue to work to "... prevent future incidents from occurring and currently are
3 implementing additional encryption solutions where appropriate."

4 18. Starbucks eventually notified the Plaintiff and the Class that their PII had been
5 stolen via a form letter dated November 19, 2008. *See* Exhibit A.
6

7 **B. Plaintiff's Actions Since Receiving the Letter from Starbucks**

8 19. Prior to having received the Notice Letter, Plaintiff had never signed up for any
9 credit monitoring services. Shortly after receiving the Notice Letter from Starbucks, Plaintiff
10 signed up for the one year of Credit Watch Service offered by Starbucks, through Experian. A
11 week or so after receiving the letter, Plaintiff called her bank and asked them to monitor her bank
12 accounts for suspicious activity.

13 20. As a result of the Starbucks data Breach, it will be necessary for Plaintiff to
14 closely monitor her personal accounts. Since receiving the Notice Letter, Plaintiff has been extra
15 vigilant about watching her banking and 401(k) accounts. Plaintiff checks these accounts nearly
16 every day and spends a substantial amount of time doing so. Prior to receiving the Notice Letter,
17 the Plaintiff only checked her bank account on a bi-weekly basis, and then only to ensure that her
18 bi-weekly paycheck had been properly deposited.
19

20 21. Furthermore, upon the expiration of the one year of credit monitoring offered by
21 Starbucks, Plaintiff will have to pay out-of-pocket for credit monitoring services she did not
22 otherwise use or need prior to the Breach.
23
24
25
26

C. Starbucks Has Acted Negligently With Employees' PII Before

22. Starbucks has a history of improperly protecting employees' PII. In 2006, Starbucks lost four laptops at its headquarters, two of which contained the PII (names, addresses, and social security numbers) of 50,000 former and 10,000 then-current employees.

23. The disappearance of the first stolen laptops was noticed on September 6, 2006, but was not reported to the public until November 4, 2006, nearly two full months after the computers went missing.

24. According to *The Seattle Times*, at the time of the 2006 loss Starbucks had a policy forbidding the storing of sensitive information, like social security numbers, on mobile equipment. In violation of its own policy, Starbucks stored PII on the laptops that were ultimately stolen. See Melissa Allison, Missing Starbucks laptops had data on 60,000 employees, contractors, *The Seattle Times*, November 4, 2006 (available at http://seattletimes.nwsources.com/html/retailreport/2008430880_retailreportdige25lap.html).

25. As a predicate to the Breach, Starbucks again violated its own supposed policies by storing Plaintiff and Class PII on a laptop, which was subsequently stolen.

D. Standard Business Practices for Ensuring Information Safety

26. Federal and state legislatures have passed a number of laws in recent years to ensure that companies protect the security of sensitive PII in the companies' files. These laws include requirements for the handling of PII by financial institutions¹ and also impose proactive obligations on companies to maintain reasonable security measures to protect the PII of individuals.

¹ The Gramm-Leach-Bliley Act, enacted on November 12, 1999, requires the FTC and other government agencies that regulate financial institutions to implement regulations to carry out the Act's financial privacy provisions. The regulations required all covered businesses to comply with the Act by July 1, 2001.

1 27. The Federal Trade Commission ("FTC") has issued a publication entitled
2 "Protecting Personal Information: A Guide for Business" ("FTC Report"), attached hereto as
3 Exhibit B. In this publication, the FTC provides guidelines for businesses on how to develop a
4 "sound data security plan" to protect against crimes of identity theft. To protect the personal
5 sensitive information in their files, the FTC Report instructs businesses to follow the following
6 guidelines:
7

- 8 (a) Keep inventory of all computers and laptops where the company stores sensitive
9 data;
- 10 (b) Do not collect PII if there is no legitimate business need. If there is a legitimate
11 business need, only keep the information as long as necessary;
- 12 (c) Use social security numbers only for required and lawful purposes and do not
13 store these numbers unnecessarily, such as for an employee or customer
14 identification number;
- 15 (d) Encrypt the PII, particularly if the sensitive information is shipped to outside
16 carriers or contractors. In addition, the business should keep an inventory of all
17 the information it ships;
- 18 (e) Do not store sensitive computer data on any computer with an Internet connection
19 unless it is essential for conducting the business;
- 20 (f) Control access to sensitive information by requiring that employees use "strong"
21 passwords; tech security experts believe the longer the password, the better; and
22 passwords; tech security experts believe the longer the password, the better; and
23 passwords; tech security experts believe the longer the password, the better; and
24 (g) Implement information disposal practices that are reasonable and appropriate to
25 prevent unauthorized access to personally identifying information.
26

1 28. In addition, the FTC Report states a number of guidelines concerning the use of
2 laptops in storing PII. As the FTC Report states:

- 3 (a) Restrict the use of laptops to employees who need them to perform their jobs;
4 (b) Assess whether sensitive PII needs to be stored on a laptop, and if not, delete the
5 information with a "wiping" program overwriting the data on the laptop;
6 (c) Consider allowing laptop users only to access sensitive information, but not to
7 store the information on their laptops;
8 (d) Require employees to store laptops in a secure place; and
9 (e) Encrypt any sensitive data contained on a laptop and configure the data so users
10 cannot download any software or change security settings without approval from
11 Information Technology specialists.
12

13 29. The FTC Report also instructs companies that outsource any business functions to
14 proactively investigate the data security practices of the outsourced company and examine their
15 standards.
16

17 30. The Washington State Office of the Attorney General in its Consumer Privacy
18 and Data Protection Report (attached hereto as Exhibit C) also provides a compilation of "best
19 practices" for protecting the personal information collected by businesses. Among those "best
20 practices":
21

- 22 (a) Maintain logs to properly track information and assure that data is only accessed
23 by authorized individuals;
24 (b) Provide adequate training for employees, agents, and contractors;
25 (c) Store the information in a secure environment (using features such as doors,
26 locks, firewalls and/or electronic security);

- (d) Take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration, and destruction;
- (e) Contain consequences for those who fail to comply with the guidelines; and
- (f) Participate in privacy seal programs and adhere to the requirements and consequences set forth by such programs.

31. As a company based in the State of Washington, Starbucks knew or should have known of the Washington State Office of the Attorney General and its Consumer Privacy and Data Protection Report.

E. Starbucks Has a Duty to Protect Employees' PII

32. Starbucks has a duty to protect employees' PII.

33. Employees' PII includes names, credit card numbers, debit card numbers, and expiration dates. Such information is a property interest owned by employees and is not owned by Starbucks.

34. Employees trust Starbucks to protect their PII for the limited purpose of working for the company. Employees expect that their PII will not be disclosed except in management of their employment.

35. Employers are also obligated to act with the care, skill, prudence, and diligence under the circumstances then prevailing that a prudent man acting in a like capacity and familiar with such matters would use in the conduct of an enterprise of a like character and with like aims.

36. Upon information and belief Starbucks failed to follow reasonable precautions to secure its employees' PII, failed to provide timely notice, and failed to protect employees from invasion of privacy, fraud, identity theft, and associated expenses.

F. Starbucks Directly Represents That It Will Protect Employee Information

37. Starbucks represents to its employees, potential employees, and customers that it will protect their sensitive PII. On its website, through which potential employees can apply to Starbucks by providing the PII, Starbucks promises to secure the information that it collects:

What type of information does Starbucks collect about me? Personal Information means information that can be used to identify an individual and includes:

name, address, phone number, e-mail address, birth date; financial information, such as credit card number; tender loaded on the Starbucks Card through agents such as Coinstar; and employment-related information, such as may be found on resumes, applications, background verification information, or in employment references.

...

How is my personal information secured? Starbucks strives to maintain appropriate physical, technical and administrative security with respect to its offices and information systems so as to prevent any loss, misuse, unauthorized access, disclosure, or modification of personal information.

We encrypt the pipe through which personal information, such as credit card numbers, is sent, using Secure Socket Layer (SSL) technology to ensure that your information is safe as it is sent over the Internet to our server.

<http://www.starbucks.com/customer/privacy.asp> (last visited Feb. 19, 2009).

G. Consequences of the Breach

38. Data breaches can lead to identity theft. The loss of a Plaintiff's PII makes the Plaintiff an easier mark for identity theft because the data lost in a data breach provides an identity thief a consolidated and verified list of actual PII. In the wrong hands, the misdeeds possible with the Plaintiff's and Class Members' PII is limited only by the imagination of the thief.

39. As defined in the Fair and Accurate Credit Transactions Act of 2003, Pub.L. 108-159, Dec. 4, 2003 (FACTA), "identity theft" is a fraud that is committed or attempted when one

1 person is using another person's identifying information without permission. Generally, identity
2 theft occurs when a person's identifying information is used to commit fraud or other crimes.
3 These crimes include credit card fraud, phone or utilities fraud, bank fraud, and government
4 fraud.

5
6 40. As the United States Government Accountability Office noted in a June 2007
7 report on Data Breaches ("GAO Report"), more than 570 breaches involving theft of personal
8 identifiers such as social security numbers were reported by the news media from January 2005
9 through January 2006. See <http://www.gao.gov/news.items/d07737.pdf> (last visited Dec. 5,
10 2008). These data breaches involve the "unauthorized or unintentional exposure, disclosure, or
11 loss of sensitive Confidential Information, which can include personally identifiable information
12 such as Social Security numbers (SSN) or financial information such as credit card numbers."

13
14 41. Identity thieves use stolen Confidential Information such as social security
15 numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and
16 bank/finance fraud.

17 42. In a pamphlet called "Identity Theft Repair Kit," the Office of the Attorney
18 General of Colorado, John W. Suthers, outlines the immediate consequences of such a breach.
19 An identity thief can then open a new credit card with the delinquent account reported on the
20 victim's credit report. The imposter changes the mailing address on the victim's credit card
21 account so that it will take some time before the victim realizes that there is a problem. The thief
22 can establish phone or wireless service in the victim's name or open a bank account and use it to
23 write bad checks. The thief can also file for bankruptcy to avoid paying debts or to avoid
24 eviction. If arrested, the thief can give the police the victim's name, affecting their criminal
25 record and subjecting the victim to arrest for not appearing in court. The thief can also make
26

1 purchases related to illegal activities or take out an auto loan. *See*

2 <http://www.ago.state.co.us/idtheft/idtrk.pdf> (last visited Dec. 5, 2008).

3 43. Identity theft crimes often include more than just crimes of financial loss. Identity
4 thieves also commit various types of government fraud, such as: obtaining a driver's license or
5 official identification card in the victim's name but with their picture; using the victim's name
6 and social security number to obtain government benefits; or filing a fraudulent tax return using
7 the victim's information. In addition, identity thieves may obtain a job using the victim's social
8 security number, rent a house or get medical services in the victim's name, and may even give
9 the victim's PII to police during an arrest resulting in an arrest warrant being issued in the
10 victim's name.
11

12 44. Victims of identity theft often have a great deal of difficulty clearing their credit
13 records, which can significantly impair their credit rating and ability to obtain loans. While law
14 enforcement, banks, credit bureaus, and collection agencies all have procedures to help identity
15 theft victims, it can still take weeks, months, or years of effort and frustration to return to normal.
16 A damaged credit history can also cause difficulty for the victim in obtaining a new job or
17 renting an apartment, as employers and landlords often review credit records of new applicants.
18
19 *Id.*

20 45. Identity theft victims spend numerous hours and money repairing damage to their
21 good name and credit record. In addition, a person whose PII has been compromised may not
22 see any signs of identity theft for years. According to the United States Government
23 Accountability Office, which conducted a comprehensive and extensive study of data breaches:
24

25 [L]aw enforcement officials told us that in some cases, stolen data may be held
26 for up to a year or more before being used to commit identity theft. Further, once
stolen data have been sold or posted on the Web, fraudulent use of that

1 information may continue for years. As a result, studies that attempt to measure
2 the harm resulting from data breaches cannot necessarily rule out all future harm.

3 See <http://www.gao.gov/news.items/d07737.pdf> (last visited Dec. 5, 2008).

4 46. Thus, Plaintiff and the Class now face years of constant surveillance and
5 monitoring to prevent further loss and damage.

6 **H. The Inadequate Remedy**

7 47. In the Notice Letter, Starbucks stated that it had “no indication that the private
8 information has been misused.” However, Starbucks provided no basis for this conclusion, nor
9 any guarantees that the information would not be misused in the future. Furthermore, since the
10 data Breach, various people have commented on Starbucks-themed internet message boards that
11 they have been victims, or know people who have been victims, of identity theft as a result of the
12 Breach.
13

14 48. Now that Starbucks has compromised the Class’s PII, Plaintiff and the Class have
15 spent and will continue to spend considerable time and money attempting to prevent and
16 monitoring for fraudulent activity on their financial accounts. According to the Washington
17 State Office of the Attorney General in its Consumer Privacy and Data Protection Report,
18 “Individual victims of identity theft spend an average of two or more years attempting to fix their
19 credit report and restore their credit status.”
20

21 49. The Notice Letter provided only a limited remedy to Plaintiff and the Class. In
22 this case the remedy Starbucks offered was credit watch services from Equifax for one year.

23 50. The Experian credit watch service offered by Starbucks is sold by Equifax as
24 “Equifax Credit Watch™ Silver” (hereinafter “Silver Package”).
25
26

1 51. The year of Silver Package credit watch services offered by Starbucks
 2 inadequately protects Plaintiff and the putative class from identity theft. Among other reasons,
 3 the remedy is inadequate because:

- 4 (a) Starbucks has only offered one year of protection.
 5
 6 (b) Starbucks only provides weekly access to credit reports, rather than the daily
 7 access that is prudent and available under "Equifax Credit Watch™ Gold."
 8 (c) Starbucks' offer leaves Plaintiff and the Class responsible for a \$250 deductible
 9 for any identity theft claims.
 10 (d) The offer fails to compensate Plaintiff and the Class for their time and resources
 11 they have and will have to expend to ensure that their credit records are not
 12 misused by the criminals who now have Plaintiff's and the Class's PII.
 13 (e) Starbucks does not offer identity restoration, which will make Plaintiff and the
 14 Class whole in case their identity has been stolen.
 15

16 52. Starbucks's failure to maintain reasonable and adequate security procedures to
 17 protect against the theft of their employees' PII has placed Plaintiff and other Class Members at
 18 an increased risk of becoming victims of identity theft crimes. In addition, Plaintiff and the
 19 Class have spent or will need to spend considerable time and money protecting themselves as a
 20 result of Defendant's conduct.
 21

22 53. Due to the fact that Plaintiff and the Class have had their social security numbers
 23 stolen as a result of Defendant's conduct, Plaintiff and the Class will now have to consistently
 24 monitor their credit card accounts, credit reports and other financial information. Social security
 25 numbers are virtually impossible to change, so Plaintiff and the Class will always be at risk for
 26 identify theft.

1 54. As a result, Plaintiff and the Class seek damages, restitution, declaratory relief,
2 injunctive relief, and any other such relief as the Court may award.

3 **VI. CLASS ACTION ALLEGATIONS**

4 55. Plaintiff brings this suit as a class action pursuant to Rule 23 of the Federal Rules
5 of Civil Procedure, on behalf of herself and all other similarly situated persons as members of a
6 Class initially defined as follows:
7

8 All persons whose PII was compromised due to the loss of Starbucks' laptop on October
9 29, 2008.

10 56. Numerosity. The proposed class is sufficiently numerous, as approximately
11 97,000 Starbucks employees have had their PII compromised. Class Members are so numerous
12 and dispersed throughout the United States that joinder of all members is impracticable. Class
13 Members can be identified by records maintained by Defendants. Plaintiff's counsel alleges
14 upon information and belief that Defendants have already contacted the approximately 97,000
15 employees whose PII was compromised when notifying the employees of the Breach.
16

17 57. Common Questions of Fact and Law. Common questions of fact and law exist as
18 to all members of the Class and predominate over any questions affecting solely individual
19 members of the Class, pursuant to Rule 23(b)(3). Among the questions of fact and law that
20 predominate over any individual issues are:
21

- 22 (a) Whether Starbucks failed to exercise care to protect Plaintiff's and the Class's PII;
23 (b) Whether Defendants owed a legal duty to Plaintiff and the Class to protect their
24 PII and whether Defendants breached this duty;
25 (c) Whether Plaintiff and the Class are at an increased risk of identity theft as a result
26 of Starbucks' failure to protect the Plaintiff's and the Class's PII;

1 (d) Whether Defendant was negligent; and

2 (e) Whether Plaintiff and members of the Class are entitled to the relief sought,
3 including injunctive relief.

4 58. Typicality. Plaintiff's claims are typical of the claims of members of the Class
5 because Plaintiff and the Class sustained damages arising out of Defendant's wrongful conduct
6 as detailed herein. Specifically, Plaintiff's and Class Members' claims arise from Starbucks's
7 failure to install and maintain reasonable security measures to protect the Plaintiff's and the
8 Class's PII.

9 59. Adequacy. Plaintiff will fairly and adequately protect the interests of Class
10 Members and has retained counsel competent and experienced in class action lawsuits. Plaintiff
11 has no interests antagonistic to or in conflict with those of Class Members and therefore is an
12 adequate representative for Class Members.

13 60. Superiority. A class action is superior to other available methods for the fair and
14 efficient adjudication of this controversy because the joinder of all Class Members is
15 impracticable. Furthermore, the adjudication of this controversy through a class action will
16 avoid the possibility of an inconsistent and potentially conflicting adjudication of the claims
17 asserted herein. There will be no difficulty in the management of this action as a class action.

18 61. Notice. Plaintiff will provide the individual notice and/or notice by publication to
19 the Class to the extent required by the Federal Rules of Civil Procedure, due process
20 considerations, and as approved by the Court.

VII. CAUSES OF ACTION

COUNT I

Negligence

62. Plaintiff repeats and re-alleges the allegations contained in each of the paragraphs of this Complaint as if fully set forth herein.

63. Starbucks had a duty to use reasonable care to protect and secure Plaintiff's and Class Members' PII within its possession or control.

64. Defendant knew or should have known of industry standards and/or "best practices" of the industry when it came to protecting the private information of employees and applicants.

65. Through its acts and omissions described herein, Defendant unlawfully breached its duty to use reasonable care to protect and secure Plaintiff's and Class Members' PII within its possession or control. More specifically, Starbucks failed to maintain a number of reasonable security procedures and practices designed to protect the PII of Plaintiff and the Class, including, but not limited to:

- (a) Using social security numbers only for necessary, required, and/or lawful uses;
- (b) Limiting access to PII to employees with a "need to know";
- (c) Encrypting any sensitive data contained on a laptop, computer network, and/or disks, as well as configuring the data so it could not be downloaded to a portable device;
- (d) Utilizing an "auto-destroy" function so that data on a computer that is reported stolen will be destroyed when the thief uses the computer;
- (e) Refraining from storing sensitive PII on a laptop;

- (f) Allowing laptop users only to access sensitive information but not to store the information on their laptops;
- (g) Requiring employees to store laptops in a secure place (using features such as doors, laptop locks, firewalls, and/or electronic security);
- (h) Providing adequate training for employees, agents, and contractors;
- (i) Implementing information disposal practices reasonable and appropriate to prevent an unauthorized access to personally identifying information;
- (j) Participating in privacy seal programs and adhering to the requirements and consequences set forth by such programs;
- (k) Imposing disciplinary measures for security policy violations; and
- (l) Creating a “culture of security” by implementing a regular schedule of employee training.

66. As a direct and proximate result of Defendant’s breach of its duties, Plaintiff and the Class have been harmed by the release of their PII, putting them at an increased risk of identity theft. Plaintiff and the Class have spent time and money to protect themselves as a result of Defendant’s conduct and will continue to have to spend time and money protecting themselves, their credit, and their reputations.

COUNT II
Breach of Contract

67. Plaintiff repeats and re-alleges the allegations contained in each of the paragraphs of this Complaint as if fully set forth herein.

1 68. Defendant came into possession of Plaintiff's and Class Members' PII for the
2 purposes of applying for and maintaining employment with Starbucks and contracted with
3 Plaintiff and Class Members to protect such information.

4 69. The contract required Defendant to safeguard and protect Plaintiff's and Class
5 Members' PII from being compromised and/or stolen.

6 70. Defendant did not safeguard or protect Plaintiff's and Class Members' PII from
7 being compromised and/or stolen.

8 71. Because Defendant failed to safeguard and protect Plaintiff's and the Class
9 Members' PII from being compromised and/or stolen, Defendant breached its contract with
10 Plaintiff and the Class Members.

11 72. Plaintiff and the Class Members suffered and will continue to suffer actual
12 damages, including, but not limited to, the cost and time spent on bank and credit monitoring,
13 identity theft, insurance fraud, anxiety, emotional distress, loss of privacy, and other economic
14 and non-noneconomic harm.

15
16
17 **PRAYER FOR RELIEF**

18 A. For an order certifying the proposed Class herein under Federal Rule of Civil
19 Procedure 23(a) and (b)(3) and appointing Plaintiff and Plaintiff's counsel of record to represent
20 said Class;

21 B. Finding that Starbucks breached its duty to safeguard and protect Plaintiff's and
22 Class Members' PII stored on its laptop lost on October 29, 2008;

23 C. Finding that Starbucks breached its contract with its employees to protect their
24 PII;
25
26

1 D. Awarding injunctive relief, including but not limited to: (i) the provision of credit
2 monitoring and/or credit card monitoring services for the Class for at least five years; (ii) the
3 provision of bank monitoring and/or bank monitoring services for the Class for at least five
4 years; (iii) the provision of identity theft insurance for the Class for at least five years; (iv) the
5 provision of credit restoration services for the Class for at least five years; (v) awarding Plaintiff
6 and Class Members the reasonable costs and expenses of suit, including attorneys' fees, filing
7 fees, and insurance for the Class; and (vi) requiring that Starbucks receive periodic compliance
8 audits by a third party regarding the security of its computer systems, specifically including
9 laptops used for processing and storing customer data, to ensure its compliance with federal and
10 industry rules, regulations, and practices;
11

12 E. Awarding the damages requested herein to Plaintiff and the Class;
13

14 F. Awarding all costs, including experts' fees and attorneys' fees, and the costs of
15 prosecuting this action;

16 G. Awarding pre-judgment and post-judgment interest as prescribed by law; and


17 H. Granting additional legal or equitable relief as this Court may find just and proper.
18

19 **JURY TRIAL DEMANDED**

20 Plaintiff hereby demands a trial by jury on all issues so triable.
21
22
23
24
25
26

1 DATED this 19th day of February, 2009.

2 KELLER ROHRBACK L.L.P.

3
4 By 
5 Lynn Lincoln Sarko, WSBA #16569
6 Mark A. Griffin, WSBA #16296
7 Gretchen Freeman Cappio, WSBA #29576
8 1201 Third Avenue, Suite 3200
9 Seattle, WA 98101-3052

10 FINKELSTEIN THOMPSON LLP
11 Mila F. Bartos
12 Karen J. Marcus
13 Eugene J. Benick
14 1050 30th Street, NW
15 Washington, D.C. 20007
16 Telephone: (202) 337-8000
17 Fax: (202) 337-8090

18
19 Attorneys for Plaintiff
20
21
22
23
24
25
26